UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

EMOTET BOTNET DISTRIBUTION SERVERS

Case No. 1:21MJ34

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the _____ District of Multiple , there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1030(a)(5)(A)	Computer Fraud
18 U.S.C. § 371	Conspiracy to Commit Computer Fraud

The application is based on these facts:

- ☑ Continued on the attached sheet.
- ☑ Delayed notice of 30 days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Blair Newman by CRA

Applicant's signature

Blair Newman, Special Agent, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone after e-mailing drafts *(specify reliable electronic means)*.

Date: 01/25/21

Judge's signature

City and state: Greensboro, North Carolina

L. Patrick Auld, United States Magistrate Judge

Printed name and title

ATTACHMENT B
PARTICULAR THINGS TO BE SEIZED

This warrant authorizes the use of remote access techniques to search the electronic storage media identified in Attachment A and to seize or copy from the electronic storage media identified in Attachment A any electronically stored information, including but not limited to web shells, used by the administrators of the Emotet botnet to communicate with and distribute files to victim computers to infect them with Emotet malware, as evidence and/or instrumentalities of the Emotet botnet computer fraud and conspiracy in violation of Title 18, United States Code, Sections 1030(a)(5)(A) (computer fraud) and 371 (conspiracy to commit computer fraud).

This warrant does not authorize the seizure of any tangible property. Except as provided above, this warrant does not authorize the seizure or copying of any content from the electronic storage media identified in Attachment A or the alteration of the functionality of the electronic storage media identified in Attachment A.

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

IN RE APPLICATION FOR A WARRANT TO SEARCH EMOTET BOTNET DISTRIBUTION SERVERS	Case No. 1:21MJ34

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41(b)(6)(B) FOR A SEARCH WARRANT

I, Blair Newman, a Special Agent with the Federal Bureau of Investigation ("FBI"), being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. The FBI is investigating the Emotet malicious software ("malware") and its associated botnet. Administrators of the Emotet botnet use a system of tiered servers to distribute the initial malware file to infected computers. Tier 1 distribution servers are typically compromised web servers with unauthorized web shells (i.e., pieces of code or scripts running on a server that enable remote administration), through which Emotet administrators upload the malware to the servers. FBI agents, analysts, and computer scientists (collectively "FBI personnel") have obtained the Emotet administrators' web shell credentials and intend to uninstall or otherwise disable the web shells on dozens of Tier 1 distribution servers located in the United States.

2. Therefore, I make this affidavit in support of an application for a warrant under Federal Rule of Criminal Procedure 41(b)(6)(B) to use remote access techniques to search Emotet Tier 1 distribution servers located in the United States, further identified in Attachment A, and to seize or copy electronically stored information that constitutes evidence and/or instrumentalities of the Emotet malware and botnet, further described in Attachment B.

3. This warrant does not authorize the collection of content of communications from the servers, nor does it authorize law enforcement officers to alter the servers' operating systems, files, or software, except as expressly provided in this affidavit.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other witnesses and agents, including foreign law enforcement officers.[1] This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 1030(a)(5)(A) (computer fraud) and

[1] This information provided by foreign law enforcement agents is reliable, based on the experience of the FBI.

371 (conspiracy to commit computer fraud) have been committed in the Middle District of North Carolina and elsewhere.

AGENT BACKGROUND

6. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since May 2019. I am currently assigned to the Cyber Squad in the Raleigh Resident Agency of the Charlotte Division. Previously, from May 2016 to May 2019, I was an FBI Staff Operations Specialist assigned to a Cyber Squad in the New York Office. I have participated in investigations of criminal offenses involving computer and wire fraud, as well as conspiracy, and I am familiar with the means and methods used to commit such offenses. I am an "investigative or law enforcement officer" within the meaning of 18 U.S.C. § 2510; that is, an officer of the United States of America who is empowered to investigate and make arrests for offenses alleged in this warrant.

STATUTORY AUTHORITY

7. Federal Rule of Criminal Procedure 41(b)(6)(B) provides that "a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if . . . (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that

have been damaged without authorization and are located in five or more districts."

8. Title 18, United States Code, Section 1030(a)(5)(A) provides that whoever "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer . . . shall be punished as provided in subsection (c) of this section." Section 1030(e)(2)(B) defines a "protected computer" as a computer "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States[.]" Section 1030(e)(8) defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information[.]"

9. Title 18, United States Code, Section 371 provides: "If two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be fined under this title or imprisoned not more than five years, or both."

PROBABLE CAUSE

A. Overview of the Emotet Malware and Botnet

10. Emotet is a family of malware that targets critical industries worldwide, including banking, e-commerce, healthcare, academia, government, and technology. Emotet malware primarily infects victim computers through spam email messages containing malicious attachments or hyperlinks. Once it has infected a victim computer, Emotet can deliver additional malware to the infected computer, such as ransomware or malware that steals financial credentials. The computers infected with Emotet malware are part of a botnet (i.e., a network of compromised computers), meaning the perpetrators can remotely control all of the infected computers in a coordinated manner. The owners and operators of the victim computers are typically unaware of the infection.

11. For example, in 2017, the computer network of a school district in the Middle District of North Carolina was infected with the Emotet malware. The Emotet infection caused damage to the school's computers, including but not limited to the school's network, which was disabled for approximately two weeks. In addition, the infection caused more than $1.4 million in losses, including but not limited to the cost of virus mitigation services and replacement computers. From 2017 to the present, there have been numerous other victims throughout North Carolina and the United States, to include

computer networks of local, state, tribal, and federal governmental units, corporations, and networks related to critical infrastructure.

12. Administrators of the Emotet botnet use a system of tiered servers, described here as Tier 1, Tier 2, and Tier 3, to distribute the initial malware file to infected computers. Tier 1 servers are typically compromised web servers belonging to what appear to be unknowing third parties. The perpetrators upload the Emotet malware to the Tier 1 servers through unauthorized web shells. The unauthorized web shells are associated with specific domains, also belonging to what appear to be unknowing third parties, which are hosted on the Tier 1 servers. Victims who click on spam email messages containing malicious attachments or hyperlinks will download the initial Emotet malware file from a Tier 1 distribution server.

13. The Tier 2 and Tier 3 servers are rented and controlled by the perpetrators. The primary function of the Tier 2 server is to forward communications containing encrypted data between the Tier 1 and Tier 3 servers.

B. Remote Access, Searches, and Seizures

14. Law enforcement officers have identified and gained lawful access to an Emotet Tier 3 distribution server located overseas. Through such access, FBI personnel have identified more than 3,600 Tier 1 distribution servers worldwide that have communicated through the Internet with the Tier 3

server during the past few weeks. Of those, more than 1,200 Tier 1 distribution servers appear to be located in the United States, according to publicly available Whois records and IP address geolocation.

15. Emotet distribution servers located in the United States constitute "protected computers" within the meaning of Rule 41(b)(6)(B) and § 1030(e)(2)(B) because they are used in or affecting interstate or foreign commerce or communication, based on their connection to the Internet. The servers have been "damaged" within the meaning of Rule 41(b)(6)(B) and § 1030(e)(8) because the installation of unauthorized web shells has impaired the integrity and availability of data, programs, systems, and information on the servers.

16. The hundreds of presumptively U.S.-based servers appear to be located in five or more judicial districts, according to publicly available Whois records and IP address geolocation. These districts include, but are not limited to, the following: District of Arizona, Central District of California, Northern District of Illinois, District of New Jersey, District of Oregon, District of Vermont, and Eastern District of Virginia.

17. In addition to identifying the Tier 1 distribution servers, FBI personnel have obtained the Emotet administrators' credentials to access the unauthorized web shells installed on those servers. FBI personnel therefore have the opportunity to use those credentials to uninstall or otherwise disable

the web shells. This warrant authorizes FBI personnel to seize or copy from Tier 1 distribution servers located in the United States any electronically stored information, including web shells, used by the administrators of the Emotet botnet to communicate with and distribute files to victim computers to infect them with Emotet malware.

18. This seizure and copying may cause the web shells to be uninstalled or otherwise disabled, but will neither alter the functionality of the servers' operating systems, files, or software, except as expressly provided in this affidavit, nor remediate malware that was already stored on the servers. However, this action is intended to prevent additional malware from being stored on the server by untethering the servers from the botnet.

TIME AND MANNER OF EXECUTION

19. I request, pursuant to Rule 41(e)(2), that the Court authorize FBI personnel to access Emotet Tier 1 distribution servers located in the United States for a period of fourteen days, beginning on or about January 25, 2021

20. Because accessing the Emotet Tier 1 distribution servers at all times will allow FBI personnel to minimize the likelihood of detection and the effectiveness of countermeasures by the administrators of the Emotet botnet that could frustrate the authorized search, good cause exists to permit the execution of the requested warrant at any time in the day or night.

DELAYED NOTIFICATION

21. I request, pursuant to Rule 41(f)(3) and 18 U.S.C. § 3103a(b), that the Court authorize the officers executing this warrant to delay notice until thirty days after the collection authorized by the warrant has been completed, including extensions. There is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of the distribution server would seriously jeopardize the ongoing investigation, as such a disclosure would likely become known to the administrators of the Emotet botnet and would give the perpetrators an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). The proposed search warrant does not authorize the seizure of any tangible property. *See* 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

22. In the event that providing notice to the subscriber or user of the infected computer no longer seriously jeopardizes the ongoing investigation, U.S. authorities will take steps to provide such notification earlier than thirty

days after the collection authorized by the warrant has been completed, including extensions.

CONCLUSION

23. I submit that this affidavit supports probable cause for a warrant to use remote access to search electronic storage media described in Attachment A and to seize or copy electronically stored information described in Attachment B.

Respectfully submitted,

/s/ Blair Newman by LPA

Blair Newman
Special Agent
Federal Bureau of Investigation

Dated: January 25, 2021

Pursuant to Rule 4.1 of the Federal Rules of Criminal Procedure, the affiant appeared before me via reliable electronic means (telephone), was placed under oath, and attested to the contents of this written affidavit.

L. Patrick Auld
United States Magistrate Judge
Middle District of North Carolina